

FREE PRACTICAL GUIDE

INTERNAL AUDIT RESOURCE LIBRARY

AUDIT PLANNING

How to Plan a Risk-Based Internal Audit

A practical guide to moving from business risk to a focused, defensible audit plan

01

Why this guide matters

How to Plan a Risk-Based Internal Audit

This guide is designed for internal auditors who need a concise, practical way to apply plan a risk-based internal audit in real engagements. It focuses on decisions, evidence and common failure points rather than theory.

THE OUTCOME YOU WANT

A practical guide to moving from business risk to a focused, defensible audit plan.

The six-step approach

- 1 Clarify why the audit matters and what decision it should support.
- 2 Identify the business objectives and risks that could prevent them.
- 3 Prioritize the risks that deserve audit attention.
- 4 Translate priority risks into audit objectives and scope.
- 5 Choose evidence, tests and resources that can answer those objectives.
- 6 Agree practical boundaries, timing and stakeholder expectations.

Steps 1-3: Build the foundation

How to Plan a Risk-Based Internal Audit

1

Clarify why the audit matters and what decision it should support.

Define the decision, risk or process question before collecting evidence. Write down what a good outcome would look like.

2

Identify the business objectives and risks that could prevent them.

Use actual transactions, system evidence, data and accountable owners to confirm how the process operates in practice.

3

Prioritize the risks that deserve audit attention.

Record assumptions, exceptions and boundaries early so later testing remains focused and reproducible.

AUDITOR PROMPT

Ask: "What evidence would convince another experienced auditor that this conclusion is reasonable?" If the answer is unclear, strengthen the planned work before moving on.

Steps 4-6: Turn work into assurance

How to Plan a Risk-Based Internal Audit

4

Translate priority risks into audit objectives and scope.

Match the depth of work to the severity of the risk. High-risk conclusions need stronger evidence and clearer documentation.

5

Choose evidence, tests and resources that can answer those objectives.

Challenge exceptions for frequency, impact, root cause and management awareness before deciding what they mean.

6

Agree practical boundaries, timing and stakeholder expectations.

Finish with an explicit conclusion and next action: no issue, improvement opportunity, finding, escalation or follow-up.

QUALITY CHECK

Before you finalize, ask whether the work directly answers the original audit question, whether evidence is sufficient, and whether a reader can understand the reasoning without being in the audit team.

WEAK APPROACH

Audit the procurement process end to end.

BETTER APPROACH

Assess whether supplier onboarding, purchase approval and payment controls manage fraud, unauthorized spend and supplier-performance risk within approved requirements.

WHY IT IS STRONGER

It links the audit to risks, outcomes and identifiable evidence.

What makes the example useful?

- It starts from a specific risk or audit question.
- It connects evidence and testing to a conclusion.
- It avoids treating process description as proof of control effectiveness.
- It leaves a clear path for management action or follow-up.

Quick reference - use this on your next audit

How to Plan a Risk-Based Internal Audit

Five practical reminders

- Planning should start with business risk, not with a recycled checklist.
- A smaller scope with clear objectives usually produces stronger assurance than a broad “review everything” approach.
- Document what is out of scope so later requests do not quietly expand the engagement.

Mini self-check

- ☐ Have I linked the work to a clear audit objective or business risk?
- ☐ Is the evidence strong enough for the importance of the conclusion?
- ☐ Have I distinguished facts, explanations and assumptions?
- ☐ Have I considered root cause and recurrence, not only the immediate exception?
- ☐ Can management understand what decision or action is required?

RESOURCE NOTE

This is a practical learning resource, not formal professional guidance. Adapt the approach to your organization, applicable standards, regulation and audit methodology.